The Collapse of the Polynomial Hierarchy: NP = P

(A Summary)

Javaid Aslam*

April 7, 2009

Abstract

We present a novel extension to the permutation group enumeration technique which is well known to have polynomial time algorithms. This extended technique allows each perfect matching in a bipartite graph on $2n$ nodes to be expressed as a unique directed path in a directed acyclic graph on $O(n^3)$ nodes. Thus it transforms the perfect matching counting problem into a directed path counting problem for directed acyclic graphs.

We further show how this technique can be used for solving a class of #P-complete counting problems by NC-algorithms, where the solution space of the associated search problems spans a symmetric group. Two examples of the natural candidates in this class are Perfect Matching and Hamiltonian Circuit problems.

The sequential time complexity and the parallel (NC) processor complexity of the above two counting problems are shown to be $O(n^{19} \log n)$ and $O(n^{19})$ respectively. And thus we prove a result even more surprising than $\mathbf{NP} = \mathbf{P}$, that is, $\#\mathbf{P} = \mathbf{FP}$, where $\mathbf{FP}$ is the class of functions, $f : \{0, 1\}^* \rightarrow \mathbb{N}$, computable in polynomial time on a deterministic model of computation. It is well established that $\mathbf{NP} \subseteq \mathbf{P}^{\#\mathbf{P}}$, and hence the Polynomial Time Hierarchy collapses to $\mathbf{P}$.

1 Introduction

Enumeration problems [GJ79] deal with counting the number of solutions in the given instance of a search problem, for example, counting the total number of Hamiltonian circuits in a given graph. Their complexity poses unique challenges and surprises. Most of them are **NP**-hard, and therefore, even if $\mathbf{NP} = \mathbf{P}$, it does not imply a polynomial solution for the for the Hamiltonian circuit enumeration problem. These problems fall into a distinct class of polynomial time equivalent problems called the #**P**-complete problems [Val79b]. As noted by Jerrum [Jer94] #**P**-hard problems are ubiquitous, those in **FP** are more of an exception. What has been found quite surprising is that the enumeration problem for perfect matching in a bipartite graph is #**P**-complete [Val79a] even though its search problem has long been known to be in **P** [Edm65].

But there is a relatively less explored result from the permutation group theory (compiled in [But91, Hof82]), concerning the enumeration of permutation groups. This result essentially says that every subgroup of the Symmetric group, S_n, can be enumerated by its generating set in polynomial time. A generating set K of a permutation group G is a subset of G such that there exists a canonic representation of each element in G as a unique product of the elements in K. A permutation group enumeration problem is essentially finding this canonic representation of the group elements such that the order of the group can also be easily computed. The generating set of any subgroup G of the symmetric group S_n consisting of $O(n!)$ permutations is known to be of size $O(n^2)$, and has a canonic representation such that the order of G can also be computed in $O(n^2)$ time. This paper makes use of these basic enumeration concepts to develop perfect matching enumeration of any bipartite graph in polynomial time.

Central to this enumeration technique is a graph theoretic model of the binary operation in a Symmetric group S_n, viz., the permutation multiplication. This model transforms a fixed generating set K of the Symmetric group S_n into a directed acyclic graph, $\Gamma(n)$ on $O(n^3)$ nodes, called the *generating graph*. The $O(n^3)$ nodes in $\Gamma(n)$ jointly represent all the generators in the generating set K. A directed edge between two nodes in $\Gamma(n)$ represents a valid multiplication of the two permutations associated with these two nodes in the implied order.

A canonic representation of each permutation π' in S_n, which is a unique product of the permutations in K, is thus transformed into a directed path in the generating graph $\Gamma(n)$. And thus each perfect matching in $K_{n,n}$ is represented by a unique directed path in the generating graph, creating its own canonic representation. Theorem 4.3 provides a specification of the perfect matching represented by a directed path in the generating graph, and Lemma 4.4 provides the criteria for that perfect matching to exist in the given bipartite graph which may not represent any subgroup of S_n.

This new enumeration technique we refer to as *permutation algebra*. We show the details in [Asl08](Sec 5) how this technique can be used to construct, not only polynomial time sequential algorithms, but also, parallel (NC [Pip79]) algorithms for the search and counting associated with the Perfect Matching and Hamiltonian Circuit problems.

Rest of this paper is organized as follows. In the Section 2 we present the definitions and basic concepts dealing with the permutation group, permutation and perfect matching. Section 3 presents the basic group enumeration technique. Section 4 describes the extended enumeration technique, the *permutation algebra*, covering a graph theoretic model of the permutation multiplication and thus provides graph theoretic analog of the generating set of S_n, leading to a generating graph for enumerating all the perfect matchings in any bipartite graph.

2 Preliminaries

A *permutation* π of a finite set, $\Omega = \{1, 2, \cdots, n\}$, is a 1-1 mapping from Ω onto itself, where for any $i \in \Omega$, the image of i under π is denoted as i^π.
The product of two permutations, say π and ψ, of Ω will be defined by $i^{\pi\psi} = (i^\pi)^\psi$.

We will use the cycle notation for permutations. That is, if a permutation $\pi = (i_1, i_2, \ \cdots \ i_r)$, where $i_x \in \Omega$, and $r \leq n$, then $i_x^\pi = i_{x+1}$, for $1 \leq x < r$ and $i_r^\pi = i_1$. Of course, a permutation could be a product of two or more disjoint cycles.

A permutation group G is a set of permutations of Ω along with the binary operation, permutation multiplication, satisfying the following axioms:

1. $\forall \pi, \psi \in G, \ \pi\psi \in G$.
2. there exists an element, $I \in G$, called the identity, such that $\forall \pi \in G$, $\pi I = I\pi = \pi$.
3. $\forall \pi \in G$, there is an element $\pi^{-1} \in G$, called the inverse of π, such that $\pi\pi^{-1} = \pi^{-1}\pi = I$.

Let H be a subgroup of G, denoted as $H < G$. Then $\forall g \in G$ the set $H \cdot g = \{h \cdot g | h \in H\}$ is called a right *coset* of H in G. Since any two cosets of a subgroup are either disjoint or equal, any group G can be partitioned into its right (left) cosets. That is, using the right cosets of H we can partition G as:

$$G \ = \ \biguplus_{i=1}^{r} H \cdot g_i \tag{2.1}$$

The elements in the set $\{g_1, g_2, \cdots, g_r\}$ are called the *right coset representatives* (AKA a *complete right traversal*) for H in G.

The group formed on all the $n!$ permutations of Ω is a distinguished permutation group called the *Symmetric Group* of Ω, denoted as S_n. Let G be a subgroup of S_n.

Let $BG = (V \cup W, E)$ be a bipartite graph on $2n$ nodes, where, $|V| = |W|$, $E = V \times W$ is the edge set, and both the node sets V and W are labeled from $\Omega = \{1, 2, \cdots, n\}$ in the same order.

A *perfect matching* in a bipartite graph BG is a set $E' \subseteq E$ of edges in BG such that each node in BG is incident with exactly one edge from E'.

Each perfect matching E' in BG represents a unique permutation π in S_n with a 1-1 onto correspondence in a natural way– for each edge $(v, w) \in E' \Leftrightarrow v^\pi = w$.

3 Group Enumeration

A permutation group enumeration problem is essentially finding a canonic representation of the group elements generated by a *generating set* such that the order of the group is also easily determined. It is somewhat similar to an enumeration problem corresponding to any search problem [GJ79] over a finite universe.

A generating set K of a permutation group G is a subset of G such that each element in G can be represented as a unique product of the elements, called *generators*, in K.

Let $G^{(i)}$ be a subgroup of G obtained from G by fixing all the points in $\{1, 2, \cdots, i\}$. That is, $\forall\, \pi \in G^{(i)}$, and $\forall j \in \{1, 2, \cdots, i\}$, $j^\pi = j$. Then it is easy to see that $G^{(i)} < G^{(i-1)}$, where $1 \le i \le n$ and $G^{(0)} = G$. The generating set K is often obtained from a sequence of the subgroups $G^{(i)}$ of G,

$$I = G^{(n)} < G^{(n-1)} < \ \cdots \ < G^{(1)} < G^{(0)} = G,$$

called a *stabilizer chain*.

Let U_i be a set of right coset representatives for $G^{(i)}$ in $G^{(i-1)}$. Then $K = \bigcup_i U_i$ is a generating set of G [Hof82]. A Group enumeration by a generating set involves a canonic representation of the group elements, i.e., a mapping f defined as

$$f : \bigtimes_{i=n}^{1} U_i \rightarrow \{\psi_n \psi_{n-1} \psi_{n-2} \cdots \psi_i \psi_{i-1} \cdots \psi_2 \psi_1 \mid \psi_i \in U_i\} = G.$$

As an example, all U_i for certain stabilizer chain of the symmetric group S_4 are shown in Table 1. All the permutations in S_4 can be expressed as a unique ordered product, $\psi_4\psi_3\psi_2\psi_1$, of the four permutations $\psi_1 \in U_1$, $\psi_2 \in U_2$, $\psi_3 \in U_3$ and $\psi_4 \in U_4$. Thus, the permutation (1,3,2,4) in S_4 has a unique canonic

U_1	U_2	U_3	U_4
$\{I, (1, 2), (1, 3), (1, 4)\}$	$\{I, (2, 3), (2, 4)\}$	$\{I, (3, 4)\}$	$\{I\}$

Table 1: The Generators of S_4

representation, $\psi_4\psi_3\psi_2\psi_1 = I * (3, 4) * (2, 4) * (1, 3)$; the element $(1, 2)$ is represented as $I * I * I * (1, 2)$. Also, note that under this enumeration scheme the order of S_4 can be found by computing the product, $|U_1| * |U_2| * |U_3| * |U_4|$.

4 Perfect Matching Enumeration

From the 1-1 equivalence of the permutations and the perfect matchings, the isomorphism of the two group, viz., S_n and the group of perfect matchings in $K_{n,n}$ is obvious. What is not obvious is an inherent mechanism in $K_{n,n}$ responsible for the multiplication of the permutations associated with the perfect matchings, and the representation of exponentially many perfect matchings by $O(n^2)$ edges. We capture this inherent mechanism in $K_{n,n}$ leading to a model of the permutation multiplication, which is succinctly described by the following Theorem [Asl08].
Let $E(\beta)$ denote a perfect matching in a bipartite graph BG' realizing a permutation $\beta \in S_n$.

Theorem 4.1. *Let $\pi \in S_n$ be realized as a perfect matching $E(\pi)$ in a bipartite graph BG' on $2n$ nodes. Then for any transposition, $\psi \in S_n$, the product $\pi\psi$ is also realized by BG' iff BG' contains a cycle of length 4 such that the two alternate edges in the cycle are covered by $E(\pi)$ and the other two by $E(\pi\psi)$.*

It is this model that leads to a graph theoretic analog of the generating set K of S_n. The following figures illustrate permutation multiplication by a transposition (2, 3) in a bipartite graph $BG' = (V, W,\ V \times W)$ on 10 nodes. For clarity, only those edges in $K_{5,5}$ that participate in this multiplication are shown in BG'.

Figure 1(a) shows a bipartite graph having two perfect matchings realizing the permutation $\pi = I$ (identity permutation) and the product $\pi\psi = I * (2, 3)$. Note that the edges v_2w_2 and v_3w_3 need not be present for the product $\pi\psi$ to be realized as a perfect matching in BG'. Figure 1(b) shows the multiplication $\pi\psi = (1, 2, 4, 3, 5) * (2, 3)$ as a cascade of two perfect matchings in two bipartite graphs. It also shows how do the edges representing the multiplier, (2, 3), depend on the multiplicand, (1, 2, 4, 3, 5).

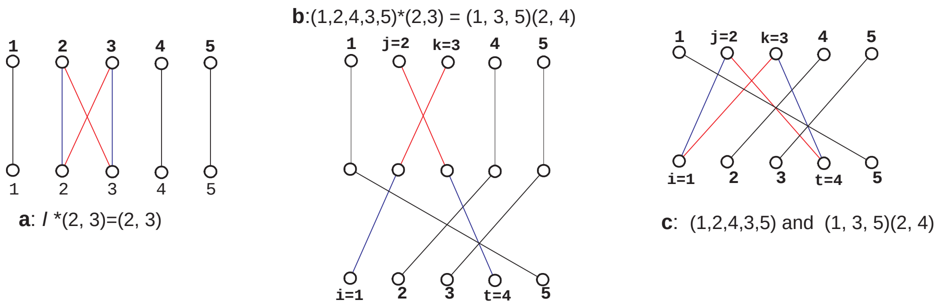

Figure 1: *The Multiplication using Perfect Matchings*

Figure 1(c) is another view of the same two permutations, (1, 2, 4, 3, 5) and $(1, 2, 4, 3, 5) * (2, 3) = (1, 3, 5)(2, 4)$, showing the two associated perfect matchings and the graph cycle, (v_1, w_2, v_4, w_3), responsible for the multiplication $(1, 2, 4, 3, 5) * (2, 3)$.

This extended enumeration technique makes use of this inherent multiplication mechanism in $K_{n,n}$, and thereby models the permutation representation, i.e. the sequence of generators, $\psi_n\psi_{n-1}\psi_{n-2}\cdots\psi_2\psi_1$, by unique directed paths in a derived directed acyclic graph called the *generating graph*, denoted as $\Gamma(n)$ ([Asl08], Defn. 4.12). This generating graph is derived from the generating set K and the complete bipartite graph $K_{n,n}$, as an application of the above Theorem 4.1. Each directed path is then further qualified by the given instance of the bipartite graph in order to determine the existence of the associated perfect matching in the given bipartite graph.

4.1 A Graph Theoretic Generating Set

We can choose the set of right coset representative for the subgroup $G^{(i)}$ in $G^{(i-1)}$ for certain fixed stabilizer chain of S_n such that U_i is of the form, $\{I, (i, i+1), (i, i+2),\ \cdots,\ (i, n)\}$. An application of Theorem 4.1 then creates a mapping between the valid product pair (π, ψ) and the graph cycle (v_i, w_k, v_t, w_i) [Figure 2]:

$$ep : \{(\pi, \psi)\} \to \{(ik, ti) |\ i^{\psi} = t^{\pi} = k\},$$

where $\pi \in G^{(i)}$, $\psi \in U_i$.

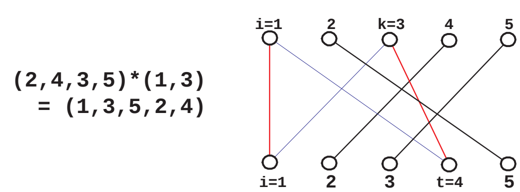

Figure 2: *Multiplication by a Coset Representative*

This mapping $ep(\pi, \psi)$ determines two unique edges v_iw_k and v_tw_i, $1 \le i < k, t \le n$, which are the two alternate edges of the graph cycle (v_i, w_k, v_t, w_i) in $K_{n,n}$ such that (ik, ti) satisfies the condition, $i^{\psi} = t^{\pi} = k$, of Theorem 4.1.

Remark 4.2. *One should note the analogy of forming the product $\pi\psi$ with the augmenting path concept in constructing a perfect matching [Edm65]. The cycle (v_i, w_k, v_t, w_i) [Figure 2], which is used to multiply π and ψ, always contains the augmenting path (v_i, w_k, v_t, w_i) corresponding to the matched edge $v_t w_k$ in $E(\pi)$.*

At each node position i in $K_{n,n}$ there are $O(n^2)$ edge-pairs corresponding to $O(n^2)$ valid values of (k,t). Thus Theorem 4.1 is used to transform the original generating set K into a graph theoretic "generating set", E_M([Asl08], Defn. 4.2) containing $O(n^3)$ edge-pairs at n node positions in $K_{n,n}$. This new generating set allows enumeration of all the perfect matchings in any bipartite graph by creating a directed acyclic graph, the generating graph $\Gamma(n)$, from E_M as follows.

4.2 The Generating Graph

The above graph theoretic multiplication of permutations also defines two different kinds of relations, viz. R and S, over the generating set, E_M. Two elements x and y in E_M are said to be related by R if the two associated generators in K can be multiplied together using the inherent mechanism in $K_{n,n}$ complying Theorem 4.1. If two elements (i.e., the edge pairs) x' and y' in E_M are (node) disjoint at the adjacent node positions in $K_{n,n}$, they are said to be related by S. The relation R is shown to be a transitive relation, and provides a basis for defining a valid multiplication path in the generating graph.

The generating graph $\Gamma(n)$ [Figure 3] models these two relations such that the nodes in $\Gamma(n)$ represent all the elements in E_M, and the (directed) solid edges indicate the relation R between the associated pairs, (x,y) in E_M, implying a valid (ordered) multiplication of the corresponding generators in K.

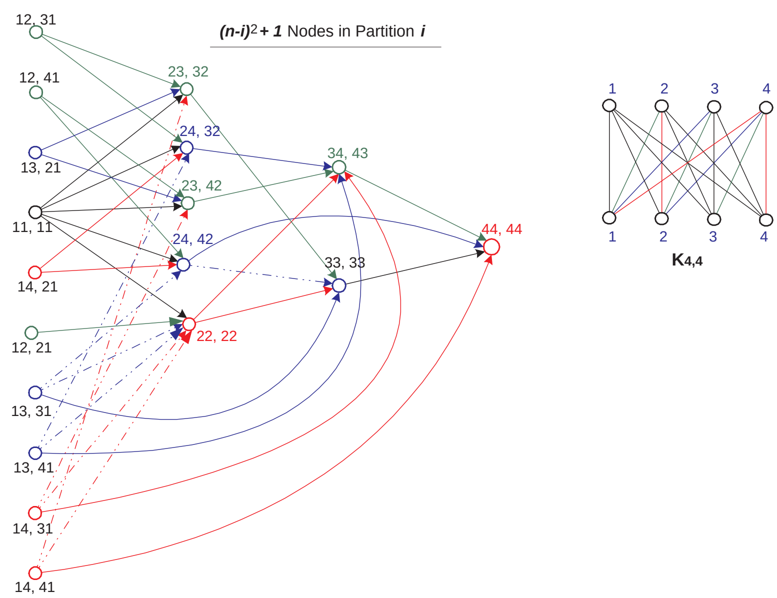

Figure 3: **The Generating Graph** $\Gamma(4)$ **for** $K_{4,4}$

All the other node pairs (x', y') in $\Gamma(n)$ exhibiting the relation S are joined by dotted (directed) edges; they get multiplied together indirectly via two disjoint R-paths to a common node in $\Gamma(n)$. A directed path in $\Gamma(n)$ is a sequence of R and S edges. When such a directed path specifies a sequence of the generators in K that can be multiplied together using $K_{n,n}$, it is called a *Valid Multiplication Path* (abbr. VMP [Asl08], Defn 4.32). Thus we are able to show how a perfect matching is represented by a VMP of length $n-1$ in $\Gamma(n)$, specifying an ordered sequence of n generators in K, which in turn represent a unique permutation in the symmetric group S_n.

To determine the existence of a perfect matching in the given instance of a bipartite graph, BG', each directed path in $\Gamma(n)$ representing a perfect matching is qualified as shown in [Figure 4].

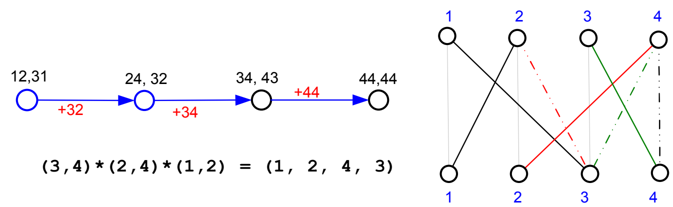

Figure 4: **Perfect Matching Composition:** *dotted edges not required*

Each of the nodes in $\Gamma(n)$ are qualified by an attribute called *edge requirement* determined by the presence of the required edges in the given bipartite graph BG' ([Asl08], Sec 4.3). There are also the surplus edges in each VMP, indicated by the dotted edges [Figure 4], which are determined by the cycle formed between the two edge pairs. For example, the dotted edge v_3w_2 is determined by the cycle (v_1, w_2, v_3, w_1) formed on the edge pairs (v_1w_2, v_3w_1) and $(v_2w_4v_3w_2)$. A VMP of length 4 in $\Gamma(4)$ is $(12, 31)(24, 32)(34, 43)(44, 44)$, and the corresponding perfect matching in BG' realizes the permutation $(1, 2, 4, 3)$.

The edge requirement of a directed path is defined using the edge requirements of the nodes and their relationship represented by the path so as to capture precisely the edges needed to realize that permutation as a perfect matching in the given bipartite graph. These edge requirements are then used to qualify all those potential directed paths which can be jointly counted as one collection (using essentially a Warshall's algorithm), having a common edge requirement and representing a set of associated perfect matchings. This in turn allows counting of all the qualified VMPs in $\Gamma(n)$, and hence all the associated perfect matchings in the given bipartite graph in polynomial sequential time, $O(n^{19}\log n)$, or in poly-logarithmic parallel (NC) time with $O(n^{19})$ processors on a PRAM [Asl08].

Two main results ([Asl08], Sec 4.4) of this enumeration technique are: (1) Theorem 4.3 which provides the specification of the perfect matching represented by a directed path in the generating graph, and (2) Lemma 4.4 which provides the criteria for that perfect matching to exist in the given bipartite graph BG'.

Let $CVMP[1, n]$ denote a directed path, which is a (complete) *Valid Multiplication Path* ([Asl08], Defn 4.33) of length $n-1$ in the generating graph $\Gamma(n)$. Note that the generating graph $\Gamma(n)$ is always fixed for a given n; what varies with the given bipartite graph is a qualifier called *edge requirements* (ER [Asl08], Sec 4.3) for each VMP.

Let BG' be a given instance of the bipartite graph on $2n$ nodes.

Theorem 4.3. *Every $CVMP[1, n]$, $p = x_1x_2 \ \cdots \ x_{n-1}x_n$ in $\Gamma(n)$, represents a unique permutation $\pi \in S_n$ given by*

$$\pi = \psi(x_n)\psi(x_{n-1}) \ \cdots \ \psi(x_2)\psi(x_1), \tag{4.1}$$

where $\psi(x_r) \in U_r$ is a transposition defined by a node x_r in $\Gamma(n)$, and U_r is a set of right coset representatives of the subgroup $G^{(r)}$ in $G^{(r-1)}$ such that $U_n \times U_{n-1} \cdots U_2 \times U_1$ generates S_n. The associated perfect matching $E(\pi)$ in BG' is

$$E(\pi) = \{e \mid e \in x_i \in p\} - \{SE(x_jx_k) \mid x_j, x_k \in p\}, \tag{4.2}$$

where SE represents a function ([Asl08], Sec 4.3) independent of BG', and determines "surplus" edges for each pair (x_j, x_k) such that x_jRx_k.

Let ER be a function that determines the edge requirements of a CVMP, p in $\Gamma(n)$, in terms of the edges in the given instance BG' of the bipartite graph.

Lemma 4.4. *Let $p = x_1x_2 \ \cdots \ x_{n-1}x_n$ be a $CVMP[1, n]$ in $\Gamma(n)$. Then $ER(p) = \emptyset \iff E(\pi)$ is a perfect matching given by Eqns. (4.1) and (4.2) in the given bipartite graph BG'.*

5 Conclusion

Let **FP** be the class of functions, $f : \{0,1\}^* \to \mathbb{N}$, computable in polynomial time on a deterministic model of computation such as a deterministic Turing machine or a RAM. Using the above two results we show in [Asl08] that the counting problem for perfect matching is not only in **FP** but in **NC** as well. Based on the fact that every $\#P$-complete problem is also NP-hard, it follows that $\mathbf{NP} \subseteq \mathbf{P}^{\#\mathbf{P}}$. And therefore, the polynomial hierarchy **PH** collapses to **P**.

References

[Asl08] Javaid Aslam, *The Collapse of the Polynomial Hierarchy: NP = P*, `http://arxiv.org/pdf/0812.1385v9`, 2008.

[But91] Gregory Butler, *Fundamental Algorithms for Permutation Groups*, Lecture Notes in Computer Science, vol. 559, Springer-Verlag, 1991.

[Edm65] Jack Edmonds, *Paths, Trees, and Flowers*, Canadian Journal of Mathematics **17** (1965), 449–467.

[GJ79] M. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman & Co., SanFrancisco, CA, 1979.

[Hof82] C. M. Hoffmann, *Group-theoretic Algorithms and Graph Isomorphism*, Lecture Notes in Computer Science, vol. 136, ch. II, Springer-Verlag, Berlin, 1982.

[Jer94] Mark Jerrum, *The Computational Complexity of Counting*, Proceedings of the International Congress of Mathematicians, Birkhauser Verlag, 1994, pp. 1407–1416.

[Pip79] N. J. Pippenger, *On Simultaneous Resource Bounds*, Proceedings of the 20th Annual Symposium on Foundations of Computer Science, October 1979, pp. 307–311.

[Val79a] L. G. Valiant, *The Complexity of Computing the Permanent*, Theoretical Computer Science **8** (1979), 189–201.

[Val79b] ———, *The Complexity of Enumeration and Reliability Problems*, SIAM J. Computing **8(3)** (1979), 410–421.

